Integrating iPhone in Enterprise

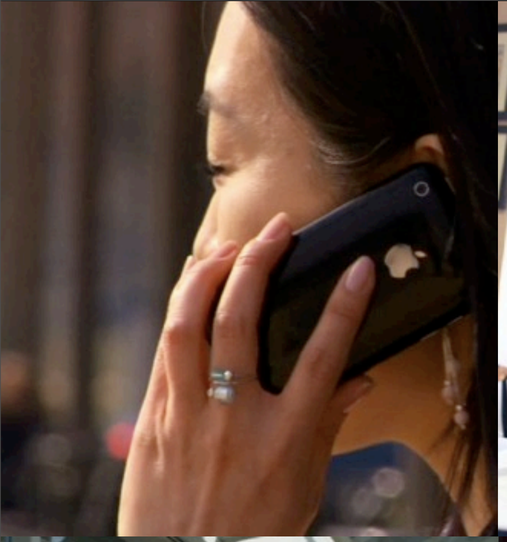
Deploying iPhone 3.0

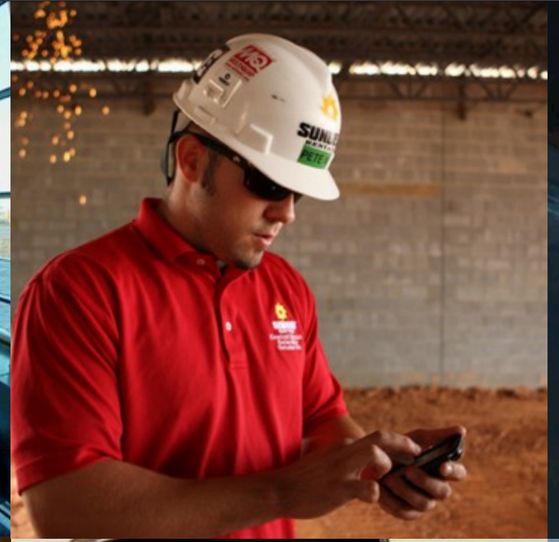
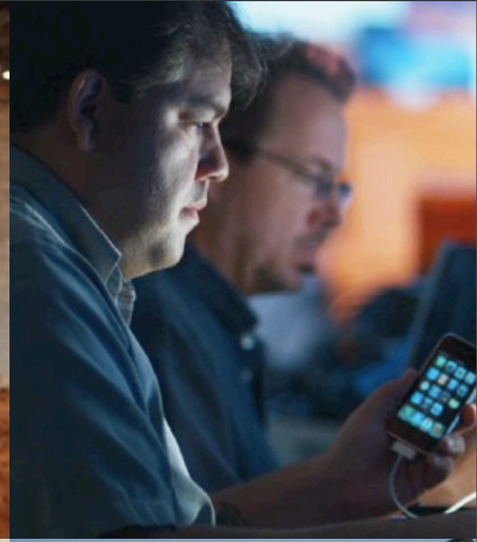
Session 601

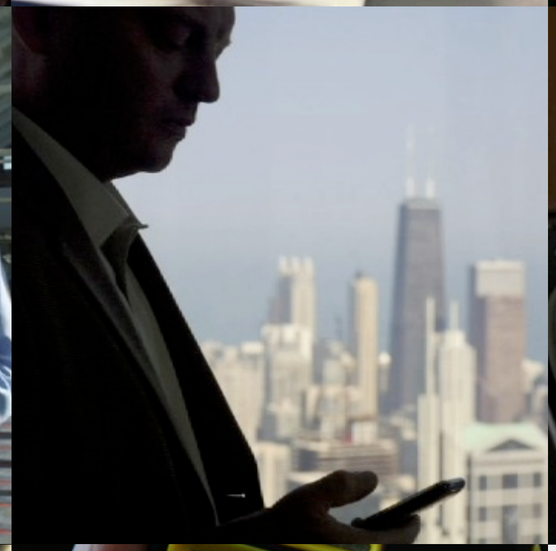
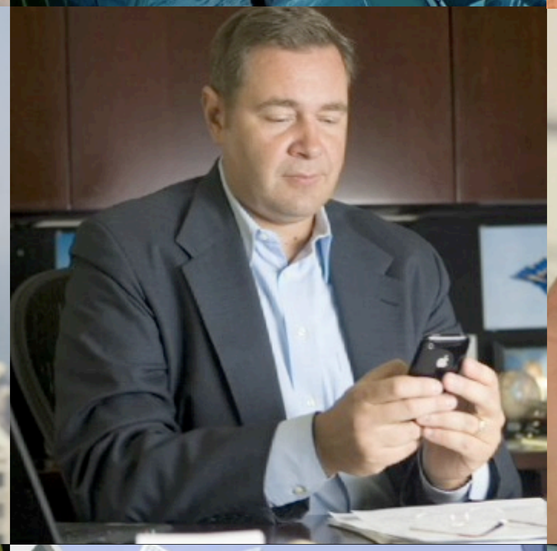
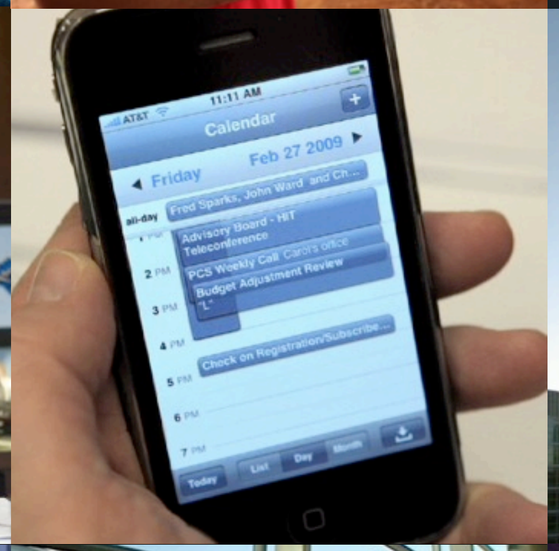
These are confidential sessions—please refrain from streaming, blogging, or taking pictures.

Integrating iPhone in Enterprise

John Wright
Core OS Software Engineering

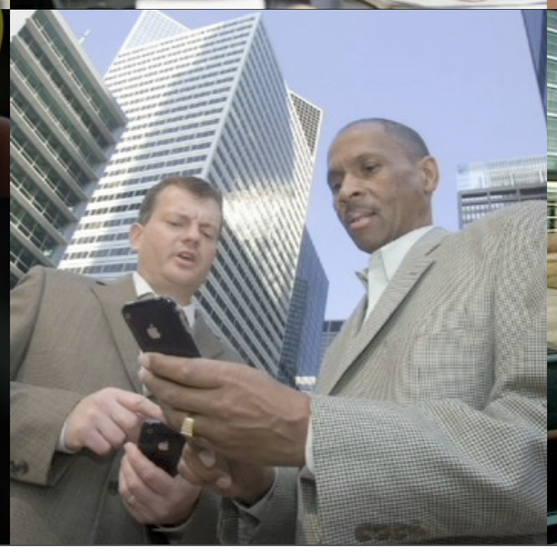
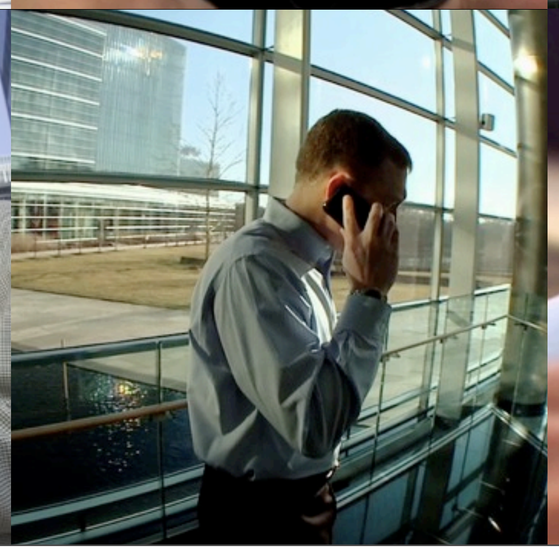
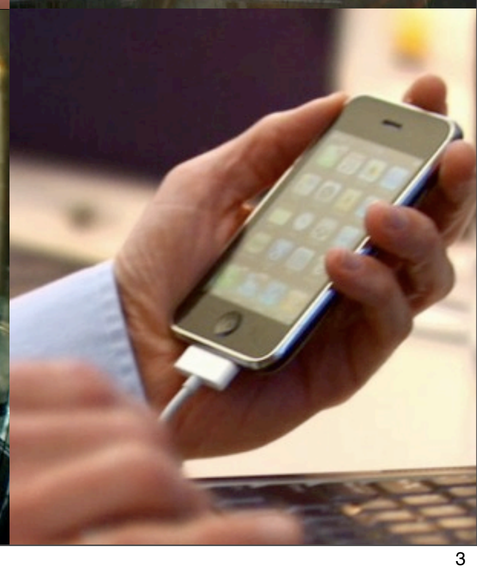





AT&T
11:11 AM
Calendar
Friday
Feb 27 2009
Fred Sparks, John Ward and Ch...
Advisory Board - HIT Teleconference
PCS Weekly Call Carols office
Budget Adjustment Review
Check on Registration/Subscribe ...
Today
List
Day
Month

USA TODAY

SUNBELT RENTALS

AT&T
2:17 PM
SUNBELT RENTALS
Mobile SalesPro
Equipment
Customers
Contracts
Leads
Settings
Help
Daily Task Planner
Due Date
Quote follow up
Meet with potential customer
04-10
New lead followup
04-10
Quote follow up call
04-13
New lead follow up
04-15
04-16




Integrate

Enterprise Infrastructure

Deploy

Configuring iPhone

Develop

In-House Applications

Integrate

Enterprise Infrastructure

Deploy

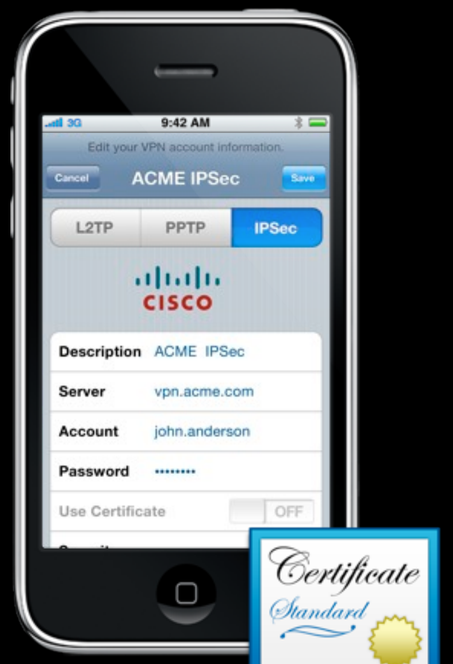
Configuring iPhone

Develop

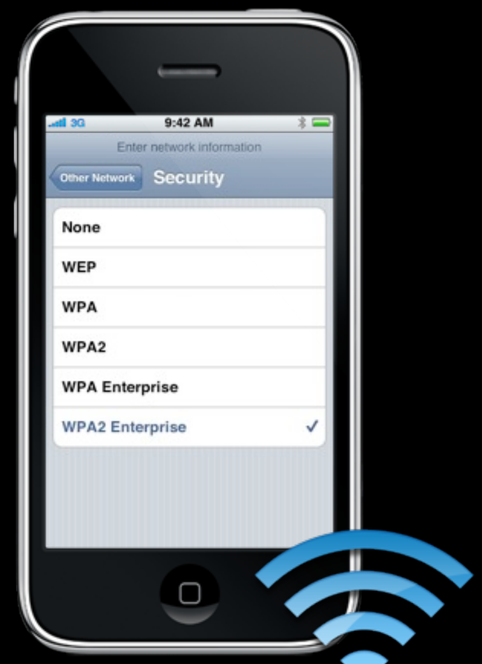
In-House Applications

Integration

Email, Calendar, Contacts



VPN



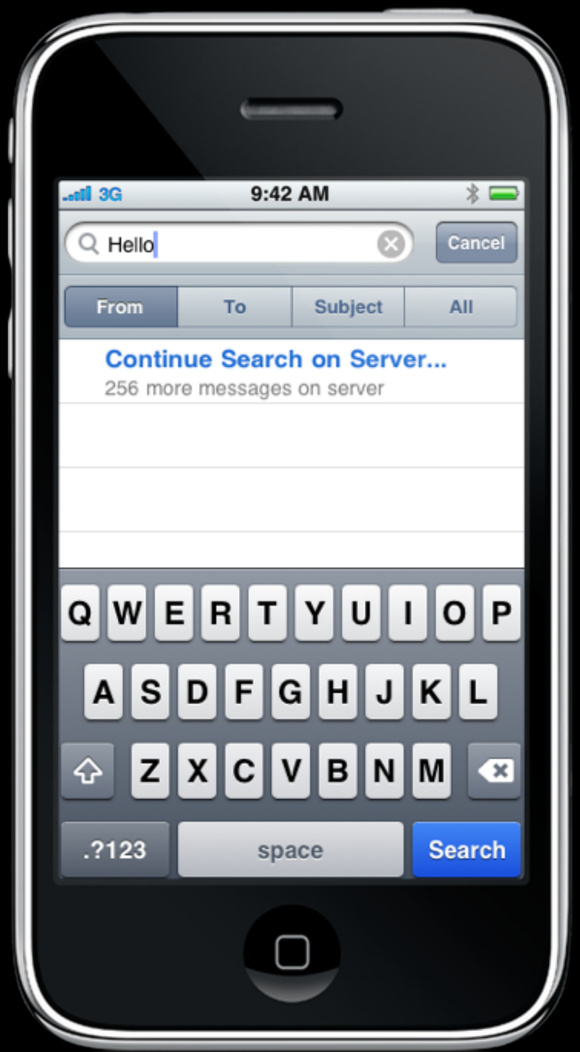
Wi-Fi

Microsoft Exchange ActiveSync

- Exchange Server 2003 SP2, 2007 SP1
- Push email, calendar, contacts
- Global Address List (GAL)
- Autodiscover (Exchange 2007)
- Remote wipe
  - Secure erase
  - Mobile Administration Web Tool (2003, 2007)
  - OWA or Exchange Management Console (2007)

Microsoft Exchange ActiveSync

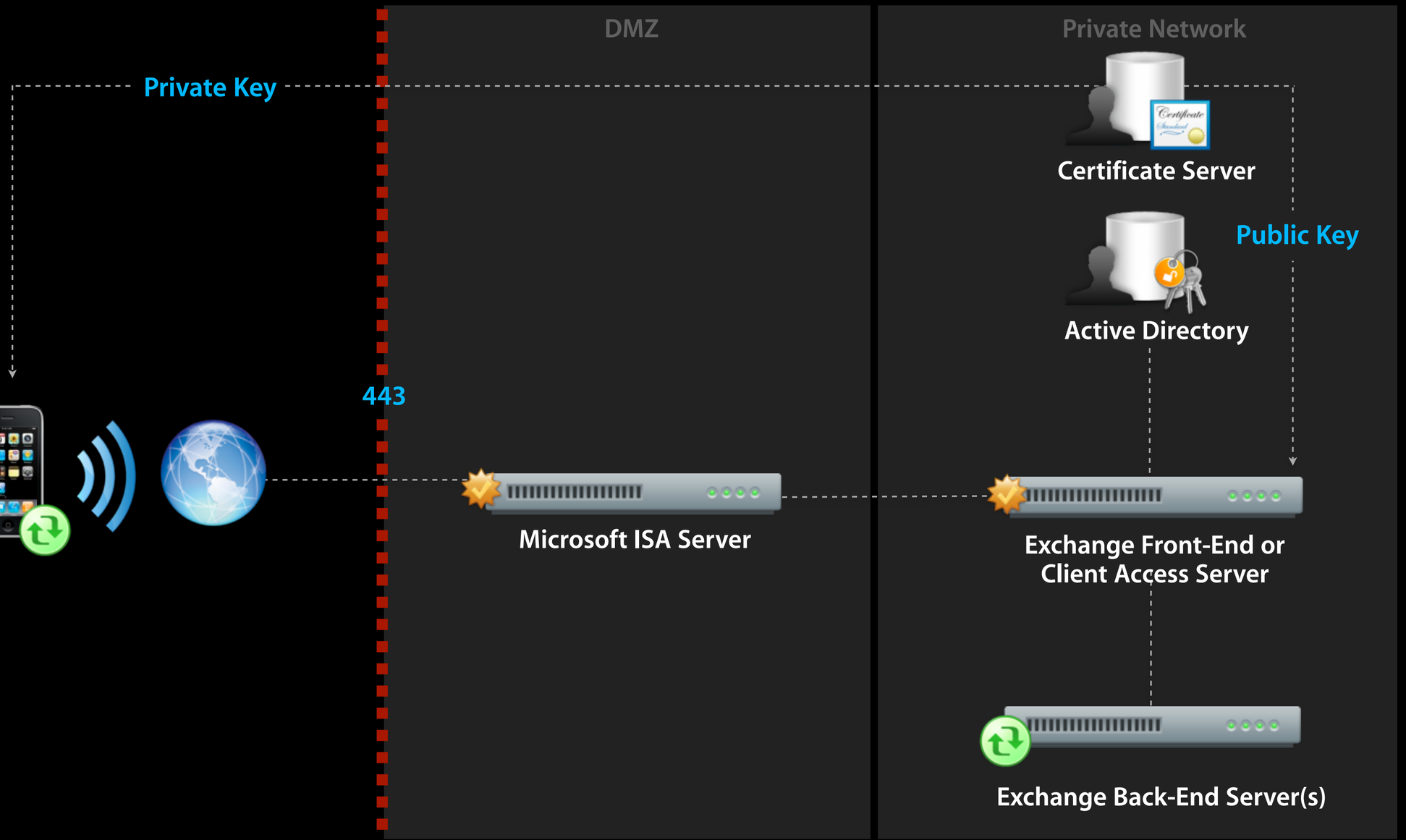
What's New 3.0



- Certificate authentication
- Enhanced policies
- Additional Exchange features
  - Search server (2007)
  - Calendar invites
  - Push to subfolders

Microsoft Exchange ActiveSync

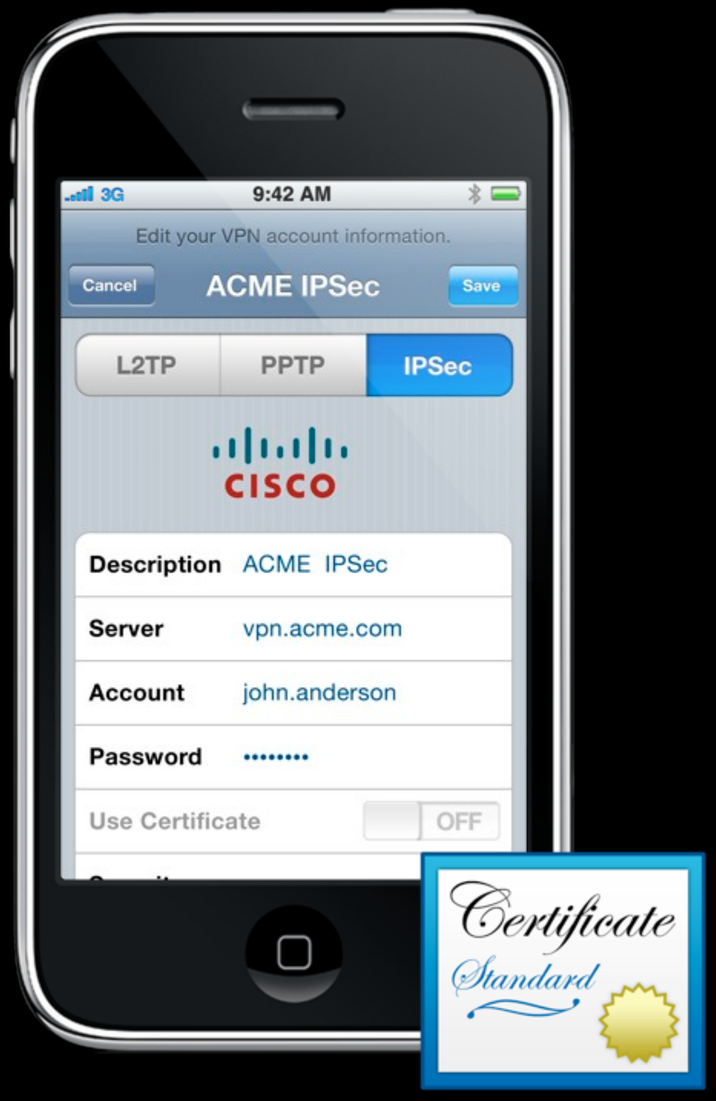
Deployment example



Standards-Based Integration

- IMAP and POP
- CalDAV 3.0
  - iCal Server, Oracle Beehive, Zimbra, Kerio, etc.
- LDAP 3.0
  - Look-up integrated with Mail, Contacts, SMS

Network Integration



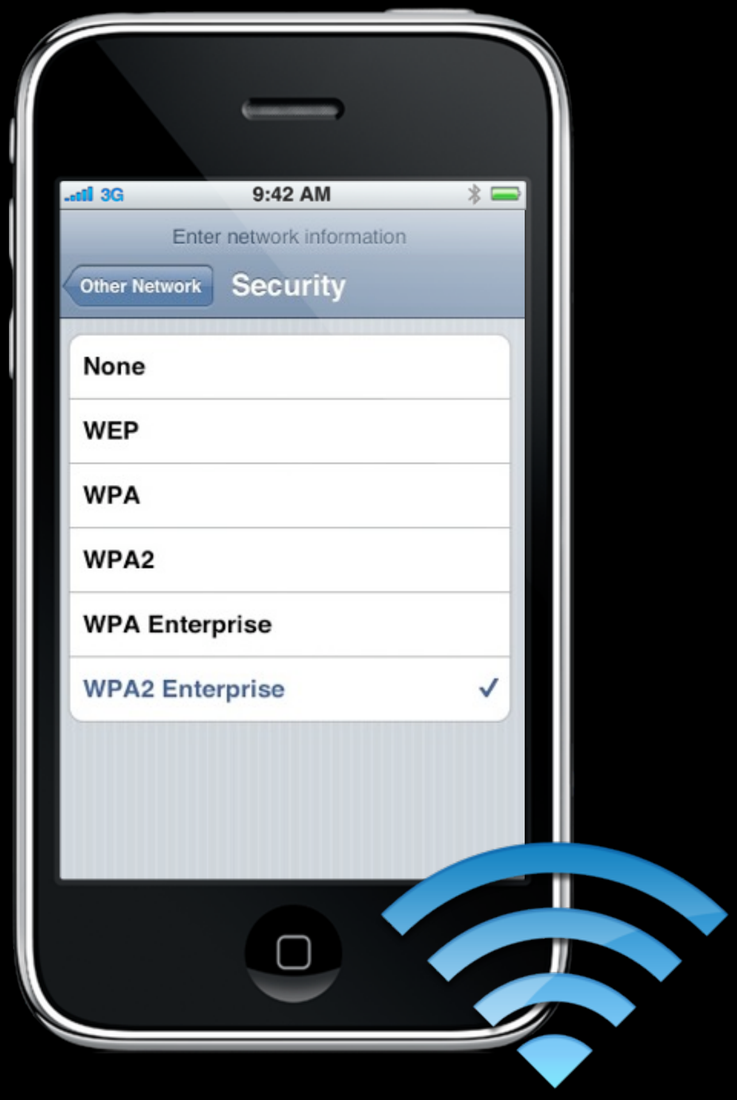
- Built-in VPN client
- Cisco IPSec, L2TP/IPSec, PPTP
- Authentication
  - Digital certificates
  - Two-factor tokens
  - Password
- VPN on demand 3.0
- Proxy support 3.0

VPN on Demand

Delivering a great user experience

- Seamless to the user
- Certificate-based authentication
  - No need for tokens
  - Runs in the background
- Based on defined domains
- Transparent to applications

Wi-Fi Security



- WPA/WPA2 Enterprise
  - 802.1x authentication
  - EAP (TLS, TTLS, FAST, SIM)
  - LEAP
  - PEAPv0, PEAPv1
- Captive network support 3.0

Integration in Practice

Duncan Keefe
Sr. Manager, Enterprise Technology Services
Apple IS&T

IS&T Web – iPhone

istweb.apple.com

Google

IS&T Web

IS&T Home | Software | Support | Accounts | Network | Training | Communication | Security

Home » Communication » Phone » iPhone

Display Prefs

- Email
- Phone
  - Phoneset
  - Voicemail
  - iPhone
- Meetings

iPhone

Using iPhone at Apple.

iPhone Preparation

Account guidance and preparation steps prior to activating iPhone.

- **Mobile Phone Accounts Overview**
  Knowing what kind of mobile account you have—or need—is important. Learn about the different account types and payment details.

iPhone Activation

- **Individual-Paid iPhone 3G Activation**
  Visit an Apple Retail or AT&T location to purchase and activate your **individual-paid** iPhone 3G.
- **Apple-Paid iPhone 3G Activation**
  Visit Apple Wireless for information on obtaining or activating your **Apple-paid** iPhone 3G.

Using iPhone

- **iPhone Security**
  Mobile devices are easily lost. It is extremely important to set a passcode lock.

  If you lose your iPhone, contact the IS&T HelpLine AND Apple Wireless immediately. The IS&T HelpLine will have your mail account password changed, and Apple Wireless will suspended service on your line, direct you to get a replacement phone, and ensure the missing device is black listed so it

Important iPhone 3G Information

iPhone 3G For Employees

iPhone Links

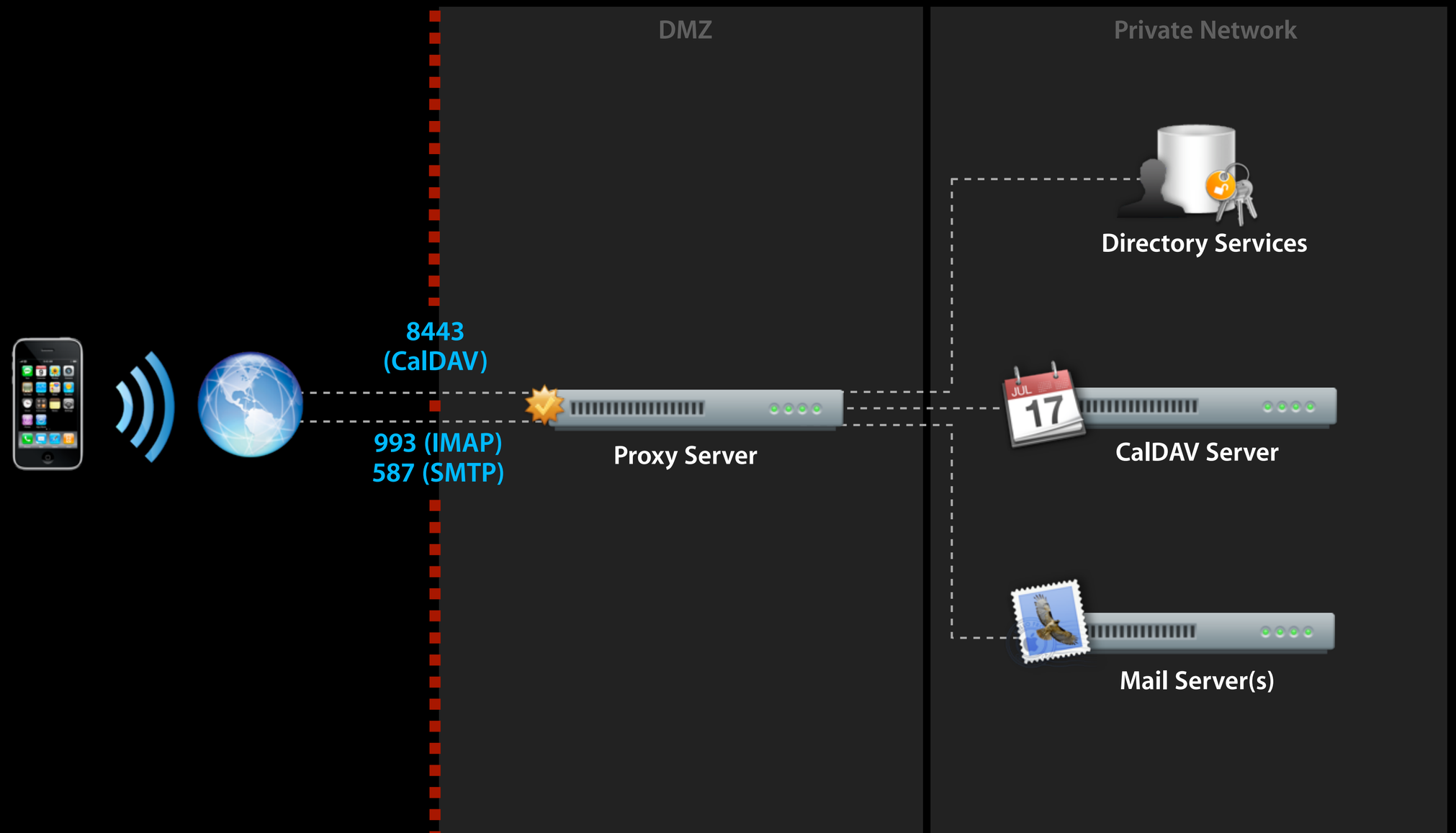
Apple Wireless
iPhone Security

iPhone on Apple.com

Apple IS&T

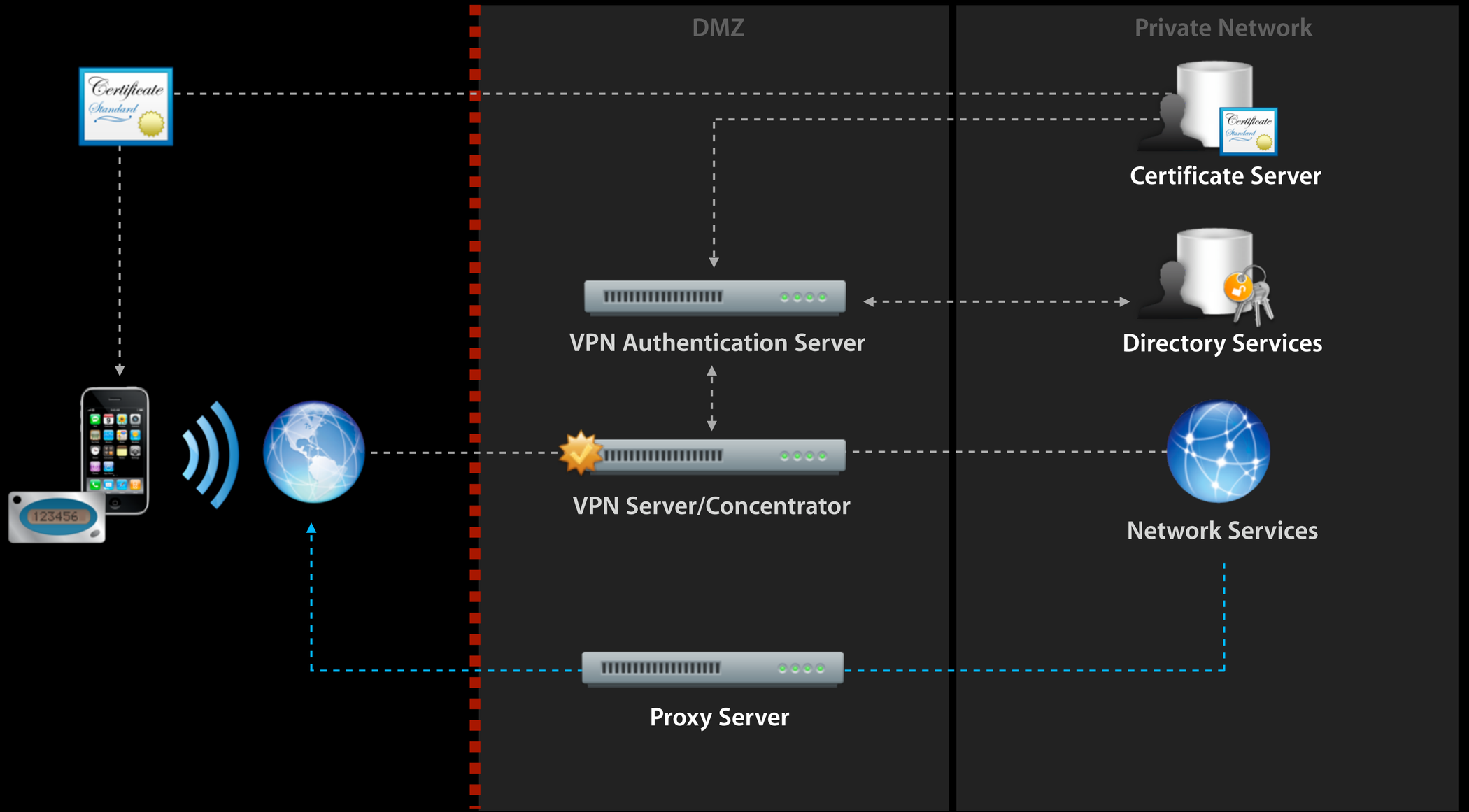
IMAP, CalDAV over SSL

Deployment example



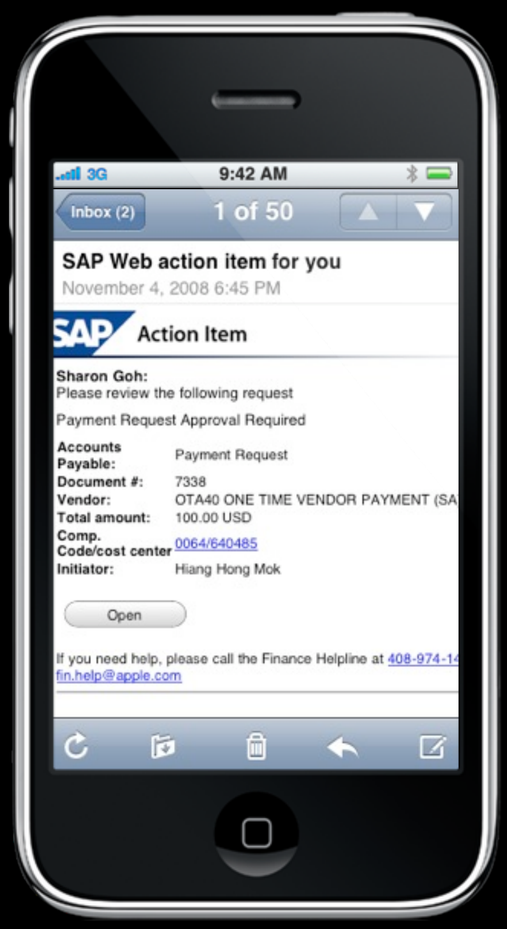
VPN

Deployment example



Integration Is Only the Beginning…

Directory



Approvals

Dashboards

Business Process

Best Practices

- Employee self service
- Documentation is key
- Streamlined network services
  - Authenticated SSL
  - Certificate VPN authentication
- Don’t stop at integration
  - In-house web, native, and hybrid apps

Integrate

Enterprise Infrastructure

Deploy

Configuring iPhone

Develop

In-House Applications

Related Sessions—Integration

Contact Management with Snow Leopard Server, Snow Leopard, and iPhone	Mission Tuesday 10:30AM
Calendaring Solutions in Snow Leopard Server, Snow Leopard, and iPhone	Mission Tuesday 2:00PM
Secure Access with 802.1X	Nob Hill Friday 2:00PM

Integrate

Enterprise Infrastructure

Deploy

Configuring iPhone

Develop

In-House Applications

Deployment Considerations

- Activation for cellular service
- Access to corporate services
- Device policies and restrictions
- Configuration of devices

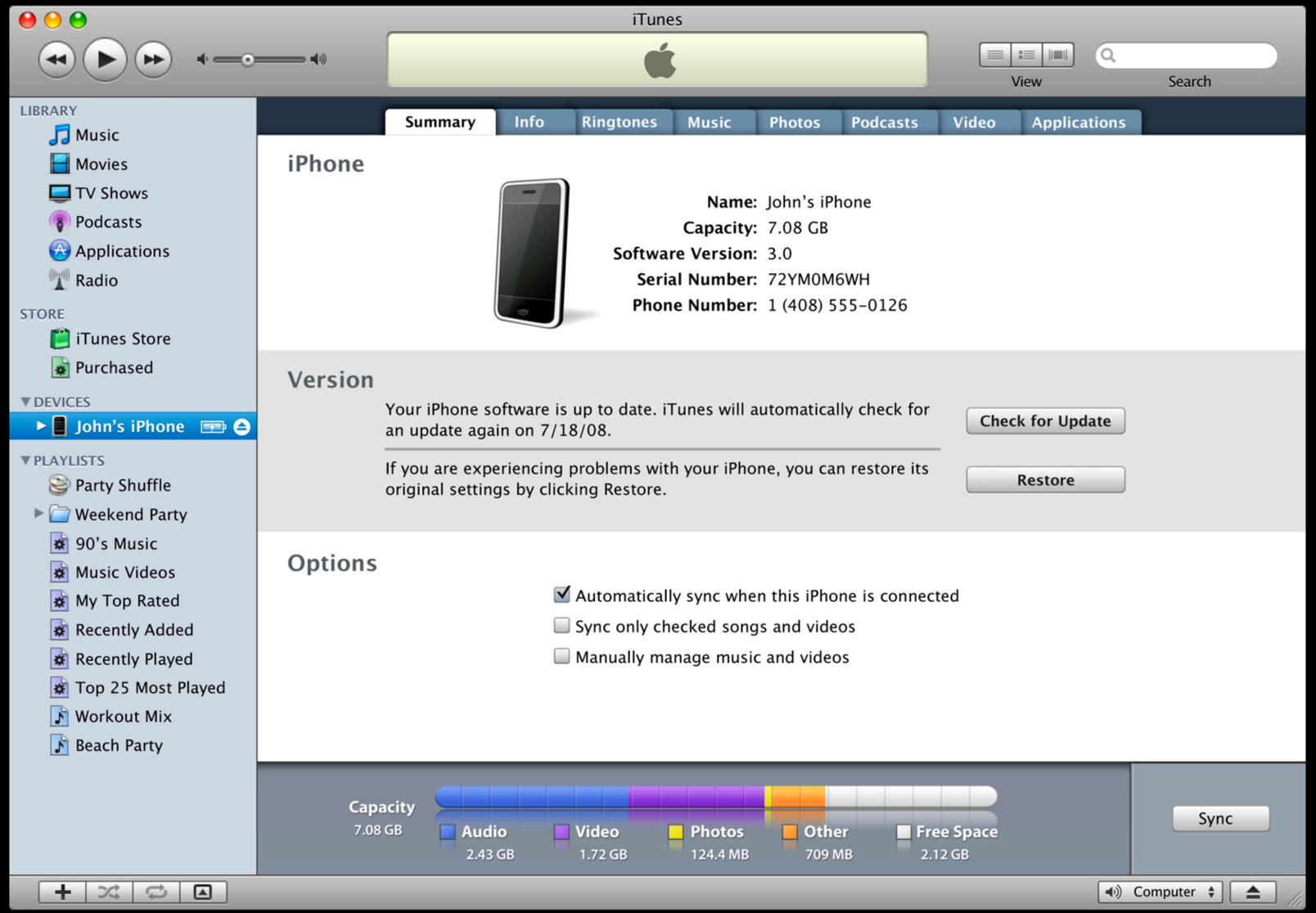
IT Organization

End Users

IT Organization

End Users

iTunes


iTunes
View
Search
LIBRARY
Music
Movies
TV Shows
Podcasts
Applications
Radio
STORE
iTunes Store
Purchased
DEVICES
John's iPhone
PLAYLISTS
Party Shuffle
Weekend Party
90's Music
Music Videos
My Top Rated
Recently Added
Recently Played
Top 25 Most Played
Workout Mix
Beach Party
Summary
Info
Ringtones
Music
Photos
Podcasts
Video
Applications
iPhone
Name: John's iPhone
Capacity: 7.08 GB
Software Version: 3.0
Serial Number: 72YM0M6WH
Phone Number: 1 (408) 555-0126
Version
Your iPhone software is up to date. iTunes will automatically check for an update again on 7/18/08.
Check for Update
If you are experiencing problems with your iPhone, you can restore its original settings by clicking Restore.
Restore
Options
Automatically sync when this iPhone is connected
Sync only checked songs and videos
Manually manage music and videos
Capacity
7.08 GB
Audio
2.43 GB
Video
1.72 GB
Photos
124.4 MB
Other
709 MB
Free Space
2.12 GB
Sync
Computer

iTunes

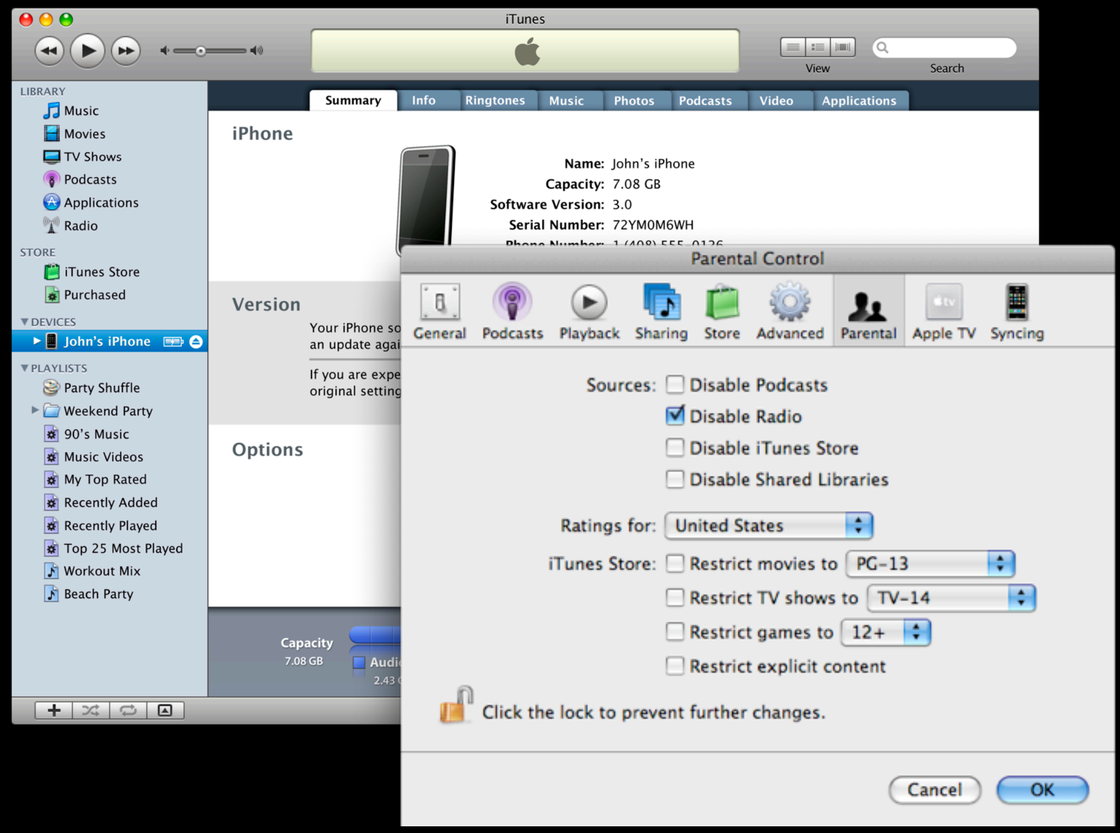
Key functions

- Device activation
- Software updates
- In-house app install
- Sync media
- Backup and restore
  - Encrypted backups 3.0

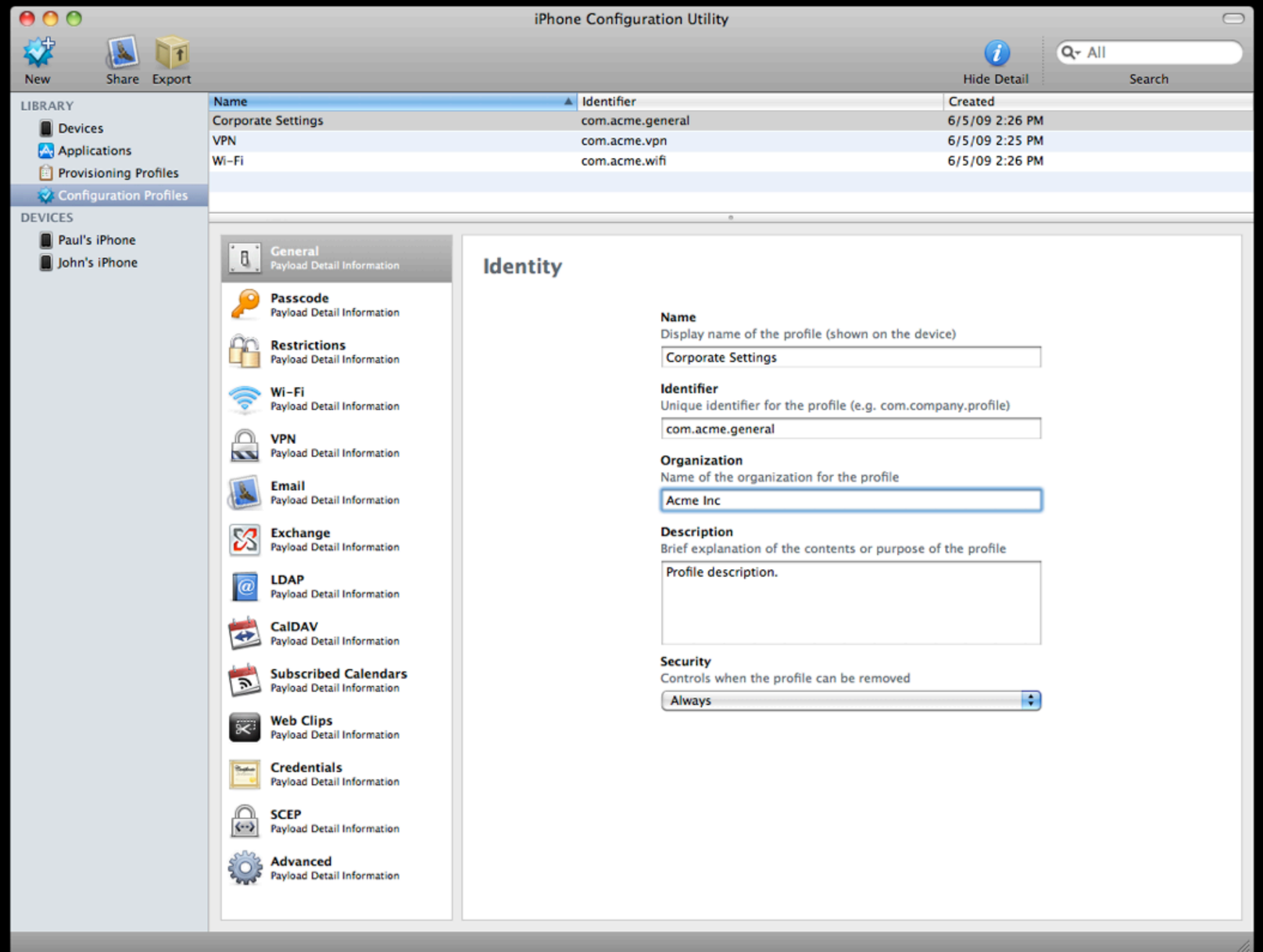
iTunes

Enterprise deployment

- Desktop management integration
- Activation-only mode
- Enterprise controls
  - Disable network services
    - iTunes store
    - Shared media libraries
  - Disable software updates
  - Disable media/data sync



iPhone Configuration Utility



iPhone Configuration Utility

What's New 3.0

- iPhone Configuration Utility 2.0
  - Additional settings
    - Restrictions
    - Prevent deletion of profiles
  - Mac and Windows
  - Sign and encrypt profiles
    - Secure settings and policies

Configuration Profiles

XML files that contain device settings and policies

Settings

- Exchange ActiveSync accounts
- IMAP accounts
- VPN settings
- Wi-Fi settings

What's New 3.0

- CalDAV accounts
- LDAP accounts
- Web Clips
- Restrictions

Restrictions

Supported device restrictions

- Allow explicit content
- Allow use of Safari
- Allow use of YouTube application
- Allow use of iTunes music store
- Allow installing apps
- Allow use of camera

Configuration Profiles

XML files that contain device settings and policies

Settings

- Exchange ActiveSync accounts
- IMAP accounts
- VPN settings
- Wi-Fi settings

What's New 3.0

- CalDAV accounts
- LDAP accounts
- Web Clips
- Restrictions
- Passcode policies (Enhanced)
- Credentials (Enhanced)

Passcode Policies

- Require passcode on device
- Allow simple values
- Require alphanumeric values
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age, in days
- Auto-lock, in minutes
- Passcode history
- Grace period of device lock
- Maximum number of failed attempts

Certificates

- Enable secure authentication and communication
  - Authentication to Exchange, VPN, Wi-Fi, other web services
  - SSL encrypted network communication
- So how do you deploy them?
  - In a configuration profile
  - Like a configuration profile via email or web
  - SCEP 3.0

Intro to SCEP

Cheryl Madson
Cisco

Intro

- This introduces SCEP as a protocol, how it came about, and how it can be used
- It is not intended to represent the details about any vendor's specific implementation

What Is SCEP?

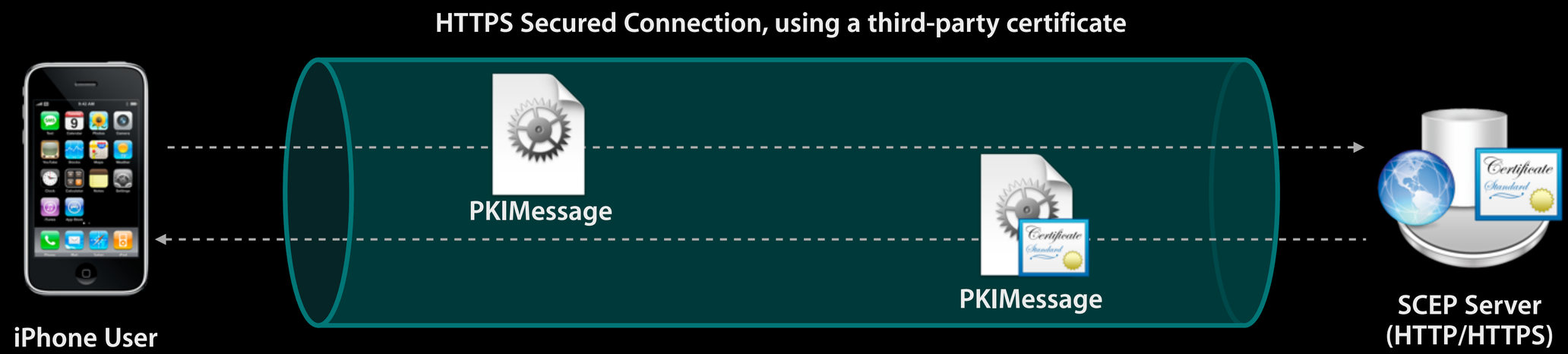
- Simple Certificate Enrollment Protocol (SCEP)
  - A protocol used for certificate enrollment
  - A lightweight mechanism for deploying certificates
    - Not a full-blown PKI management solution
- Protocol originally developed by Verisign for Cisco
  - IETF PKIX standards effort had two major competing proposals (MS vs. Entrust)
  - SCEP is maintained by Cisco as an IETF Internet Draft

What Problem Does It Solve?

- Original problem: Supply certificates for routers running IPSec
  - A router is not a host with browser software
  - A router doesn't have pre-installed CA certs/trustpoints
  - Bootstrap issue: How to obtain device certificates without pre-established trust relationship?

SCEP Protocol Basics: Transport

- SCEP is defined over HTTP
- iPhone runs SCEP over HTTPS
- The HTTPS session is secured by a trust point already known to iPhone (pre-installed root)—*Not the enterprise CA*



SCEP Protocol Basics: PKImessage

Does not inherently depend on transport for security

PKIMessage

=

A PKCS#7 signed by the sender. It contains:

A PKCS#7 encrypted to the recipient. Which in turn contains:

Usually either:

- **A PKCS#10 Certificate Request**
  - **Including the ChallengePassword**
- **An X.509 Certificate response**

- **Control messages such as "PENDING", "REJECTED", "SUCCESS", etc**

SCEP Protocol Basics: Infrastructure Models

Two primary models

Certificate Authority
SCEP Server

1. CA takes on all of SCEP server functionality—authorizing clients, validating enrollment requests and issuing certificates

Registration Authority + Certificate Authority

2. CA issues certificates; RA, in its role as intermediary between the client and CA, is responsible for the other tasks; RA can be placed in DMZ

Cisco IOS CA Server supports both models
Microsoft CA Server (with SCEP extensions) supports only RA/CA model

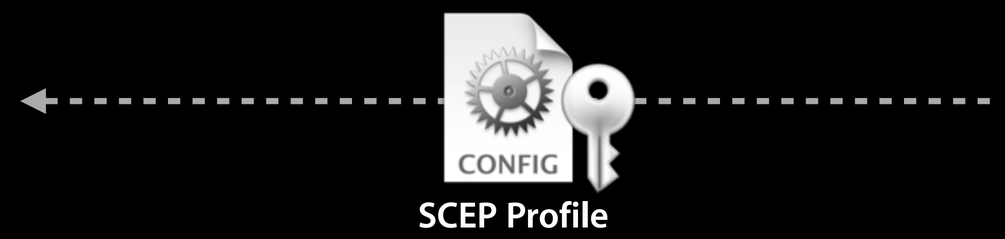
Authorizing User Requests

Establishing client credentials

- SCEP should integrate with existing authorization services
  - Client certificate credentials can replace other credentials (e.g. userid/password)
- Two methods supported on iPhone
  - Based on one-time password (OTP)
  - Based on username and password
- Profile Web Service
  - Authorizes iPhone clients
  - Delivers profile for client to initiate enrollment request

Authorization—One Time Password

Authentication



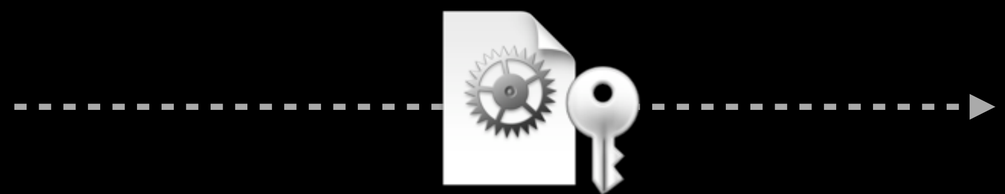
SCEP Profile

Profile Web Service

Directory Service

One Time Password is generated and inserted into SCEP profile:

<key> Challenge Password </key>

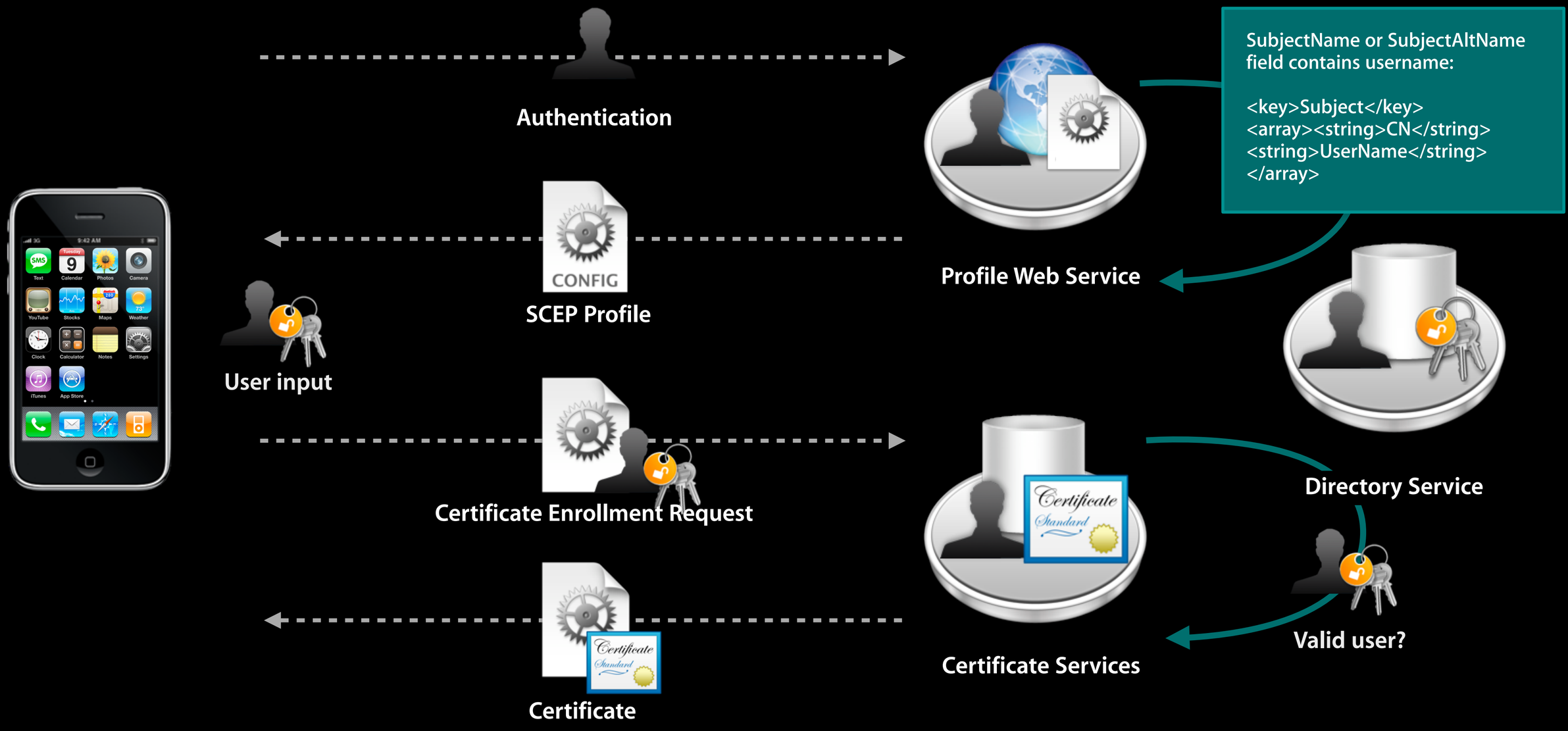


Certificate Enrollment Request

Certificate Services

Certificate

Authorization—Username Password



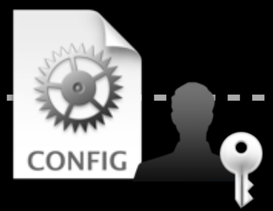
Cisco IT iPhone Pilot (Conceptual)

Authentication

Profile Web Service

Encoding of username into certificate

Directory Service



CONFIG

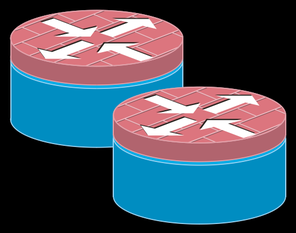
SCEP Profile

One Time Password is generated and inserted into SCEP profile

Certificate Services

Certificate Enrollment Request

Valid User?



Certificate

Cisco IPsec VPN

Valid Certificate?

For Further Information

- SCEP protocol—current I-D is draft-nourse-scep-18
- New version available soon
- This spec is an individual submission; The goal is to publish as an RFC but not as a standards track document
- Document has recently been evaluated by the IETF Security Area Directorate

Summary

User Authentication

- Ensures that the user is authorized prior to proceeding with certificate enrollment

Certificate Enrollment

- Generates a standard certificate signing request (PKCS#10) which is also encrypted (PKCS#7) via the SCEP protocol (PKIMessage)
- Receives the identity certificate (x.509) in response

Over-the-Air Device Configuration

- Delivers an encrypted configuration profile with the settings and credentials for iPhone to connect to corporate services (Exchange, VPN, Wi-Fi, etc.)

Over-the-Air Configuration

Configuration Profile Request
(Pre-Enrolled Certificate)

Profile Web Service

Directory Service

Encrypted
Configuration Profile

Decrypted
Configuration Profile

Infrastructure Requirements

Directory Service

- Authenticates users

Certificate Service (CA)

- Supports SCEP
- Authorizes user requests
- Delivers certificates

Profile Web Service

- Hosts HTTPS session
- Generates config profiles
- Signs and encrypts profiles
- Tracks user requests
- Proxy/RA (optional)

Related Sessions—Deployment

iPhone Configuration Creation and Deployment	Pacific Heights Thursday 3:30PM
iPhone Configuration Creation and Deployment Lab	Information Technologies Lab Thursday 5:00PM
iPhone Security Best Practices	Mission Wednesday 5:00PM
iPhone OS Security Lab	iPhone Lab D Thursday 5:00PM

Integrate

Enterprise Infrastructure

Deploy

Configuring iPhone

Develop

In-House Applications

3G
9:42 AM
Text
Calendar
Photos
Camera
YouTube
Stocks
Maps
Weather
Clock
Calculator
Notes
Settings
iTunes
App Store
Phone
Mail
Safari
iPod
50,000 apps

Secure Platform

- Signed and sandboxed applications
  - Ensures app integrity
  - Restricts access to data of other applications
- Security Framework and Keychain Services
  - Certificate, Key, and Trust Services
  - Safely stores credentials
- iPhone 3G S—hardware encryption
  - Encrypted data at rest
  - Instantaneous remote wipe

Your business is unique

Mobile Apps for Mobile Workers

- Specific tasks for mobile situations
- When your users are on the move
- Minimal input, maximum output
- Streamlined workflow
- Optimized for ease of use
- Integrated with your data and the network

MULTIQUIP
PETE

Development in Practice

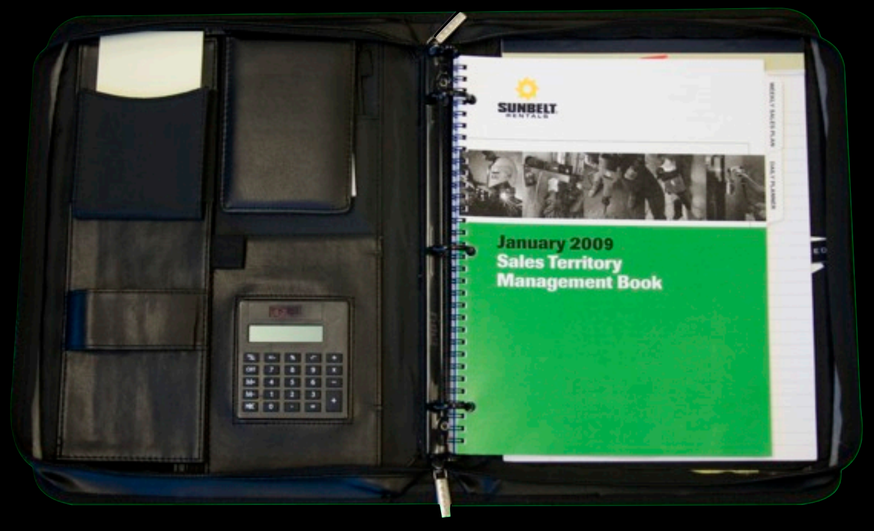
Dean Moore
Sr. Systems Manager and Architect
Sunbelt Rentals

Who We Are

- Sunbelt Rentals is a wholly owned subsidiary of Ashtead Group plc
- Publicly traded in the UK (AHT.L)
- Third largest equipment rental company in the US, second in the world
- Over 400 locations in 34 states and the District of Columbia
- 5500 Employees; sales force of 800
- Two iPhone developers

Where We Were

- Primary device used by the sales force was a Sprint/Nextel two-way radio
- Communication to field via conference calls
- Customer data printed in book format and distributed quarterly
- No access to operational data while on sales calls
- Limited access to new sales lead data



Where We Needed to Be

- Improve communication within the company
- Move sales force from manual procedures to technology based systems
- Provide sales force with live pertinent information at the point of sale
- Integrate multiple disparate systems
- Provide better customer service

How Did We Get There?

Microsoft®
Exchange

- Mail
- Calendar
- Contacts (GAL)

SUNBELT® RENTALS
Mobile SalesPro

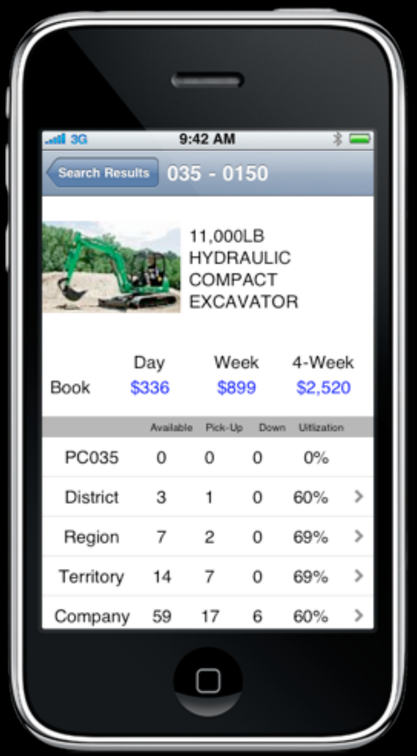
- Equipment
- Customers
- Contracts
- Leads

Mobile Sales Pro

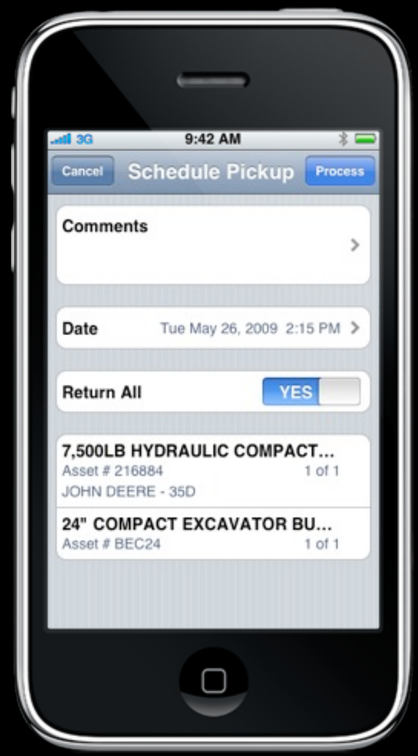
Complete mobile workflow

Plan
- Daily task planner
- Sales leads
- Share leads
- CRM integration

Prep
- Customer account detail
- Current AR status
- Rental history
- Equipment on rent



Fullfill
- Real-time needs analysis
- Equipment availability
- Current rates
- Equipment location

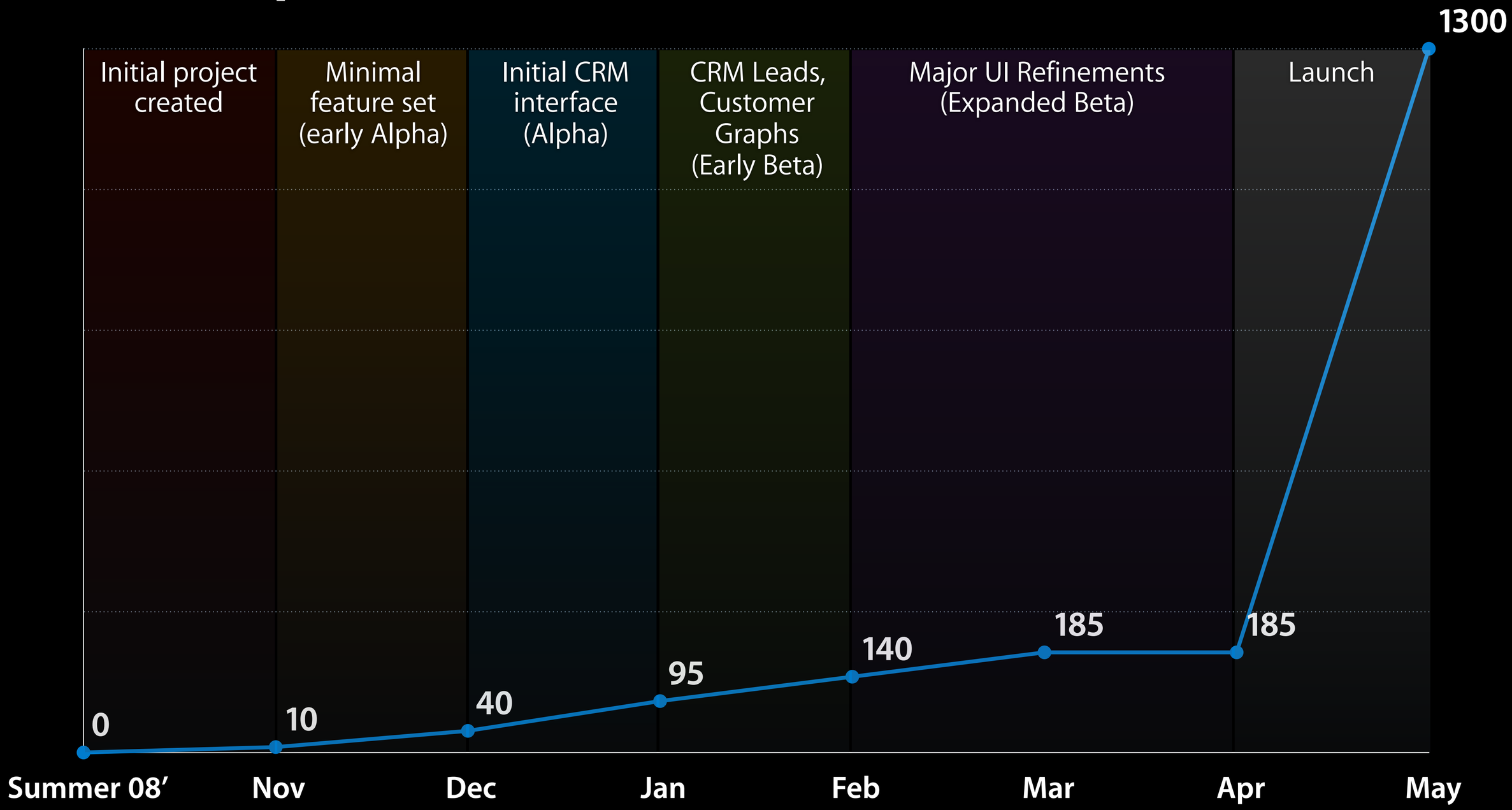


Service
- Email credit application
- View/email rental contracts
- View/email invoices
- Request pickup

Our Development Process

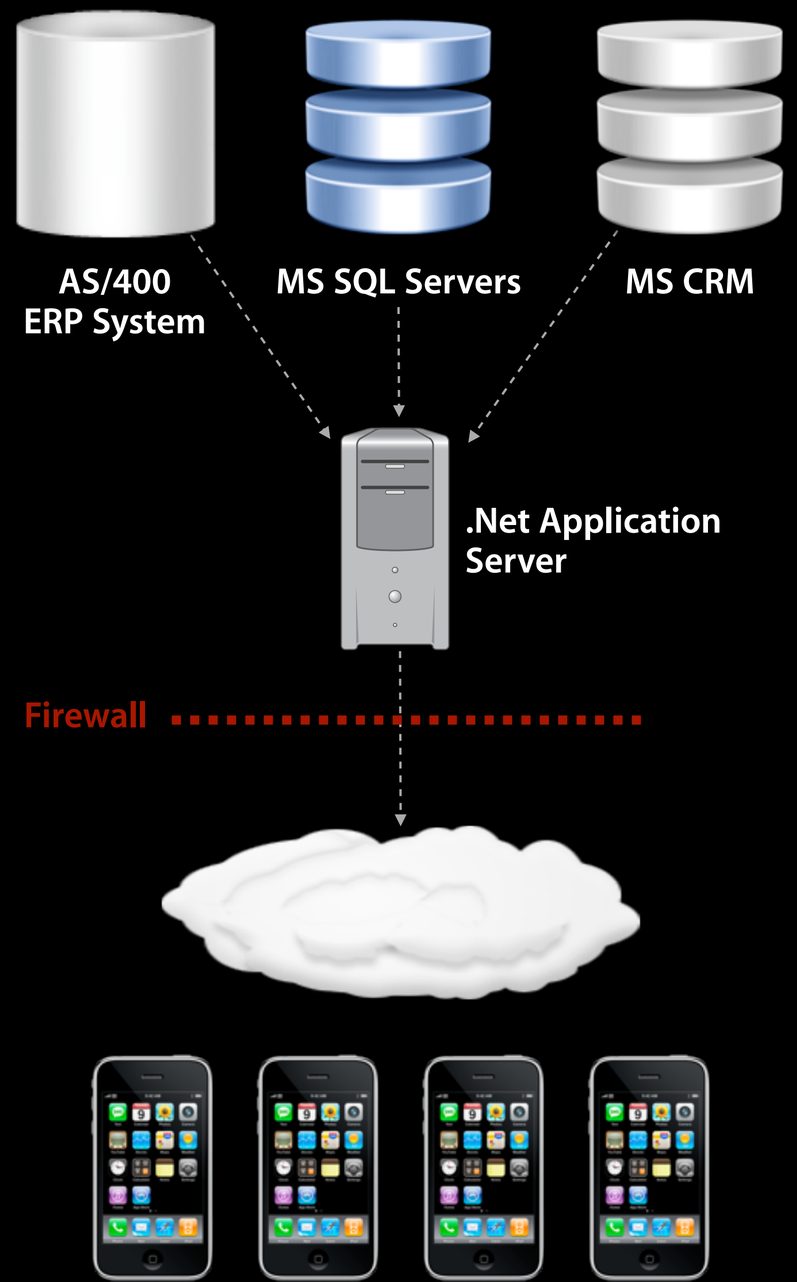
- Simplified project life cycle
- Defined goals and milestones
- Created rough screen layouts
- Direct communication from developer to sales force

Development Timeline



How We Get the Data

- C# .NET Web Services on our application server
- MS SQL stored procedures, MS CRM API and AS/400 RPG programs
- Data transmitted as XML via HTTPS
- Homegrown SOAP wrapper class and XML parser
- Custom security model



Best Practices

- Involve users early in development process and listen to their feedback
- Well defined and agreed upon feature set
- Develop and deploy in phases
- Follow the UI guideline
- Architect once; leverage often

Related Sessions—Development

iPhone Web Applications from Start to Finish	Russian Hill Tuesday 2:00PM
Creating Secure iPhone and Mac OS X Applications	Russian Hill Tuesday 5:00PM
In-House App Development for iPhone	Mission Tuesday 5:00PM

Integrate

Enterprise Infrastructure

Deploy

Configuring iPhone

Develop

In-House Applications

Thank You!

WWDC Session Survey

You can rate your sessions on the WWDC Attendee Site.

Survey forms are located on each session description page at:

developer.apple.com/wwdc/attendee

WWDC09